UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,344	08/16/2001	Massimiliano Antonio Poletto	RIV-0420	2635

87555 7590 01/29/2010

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
01/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MASSIMILIANO ANTONIO POLETTO and
EDWARD W. KOHLER, JR.

Appeal 2009-006256
Application 09/931,344
Technology Center 2400

Decided: January 29, 2010

Before KENNETH W. HAIRSTON, MARC S. HOFF, and
BRADLEY W. BAUMEISTER, *Administrative Patent Judges*.

BAUMEISTER, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF CASE

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1-39. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Appellants' invention relates to a computer-system architecture for thwarting denial of service attacks on a victim data center. The system includes a control center that communicates with and controls gateway devices and data collectors. The gateways and data collectors are types of monitors that monitor and collect statistics on network traffic. The gateway devices may be located at the edges of the internet at the entry points of the victim data centers. The data collectors may be disposed at various points in the network. The central controller analyzes network traffic statistics received from the gateways and monitors to identify malicious network traffic. (Abstract; Spec. 5).

Independent claim 1 is illustrative, reading as follows:

> 1. A gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises:
>
> a computing device comprising:
>
> a monitoring process that monitors network traffic through the gateway;
>
> a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; and
>
> a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack.

The Examiner relies on the following prior art references to show unpatentability:

Pearson	US 6,990,591 B1	Jan. 24, 2006 (filed Dec. 22, 1999)
Cheriton	US 7,120,931 B1	Oct. 10, 2006 (filed Aug. 31, 2000)

Claims 1, 16, and 29 stand provisionally rejected on the grounds of non-statutory double patenting over claims 1, 9, 18 and 21 of co-pending Application No. 09/931,291 (now US Patent 7,278,159, issued to Kaashoek).

Claims 1, 16, and 29 stand provisionally rejected on the grounds of non-statutory double patenting over claims 1, 3, and 4 of co-pending Application No. 10/066,252 (now US Patent 7,657,934, issued to Poletto).

Claims 1-39 stand rejected under 35 U.S.C. § 103(a) as obvious over Pearson in view of Cheriton.

Appellants do not provide any arguments in relation to either of the two non-statutory double patenting rejections (App. Br. 7).[1] Accordingly, we summarily affirm the Examiner's decision rejecting claims 1, 16, and 29 over each of Kaashoek and Poletto.

With respect to the obviousness rejection under 35 U.S.C. § 103, the Examiner finds that Pearson discloses every limitation of claim 1 except for

[1] Rather than repeat the arguments of Appellants or the Examiner, we refer to the following documents for their respective details: (1) the Appeal Brief ("App. Br."), filed October 24, 2007; (2) the Examiner's Answer ("Ans."), mailed February 6, 2008; and (3) the Reply Brief ("Reply Br."), filed April 4, 2008. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

a filtering process to insert filters on network devices (Ans. 8-9). The Examiner further finds (1) that Cheriton teaches this missing limitation and (2) that motivation existed to combine Cheriton's teachings regarding the network filtering with Pearson's monitoring system (Ans. 9). The Examiner further finds that the act of Pearson's gateway communicating a signal to a remote monitoring center (RMC) "obviously suggests sending statistics in the signal collected in the gateway to [a control center]" because Pearson's "gateway communicating a signal to the control center (RMC) is not merely for signaling an alert, but is a message with statistics indicative of an attack" (Ans. 22). The Examiner also asserts that Pearson's acts of transmitting wake-up signals and violated rules to the RMC suggest sending information "to the RMC for inspection and not just a mere signaling to alert the RMC" (Ans. 22-23).

Appellants argue, *inter alia*, that Pearson fails to teach a communication process wherein a gateway communicates statistics to a control center (App. Br. 3-11; Reply Br. 2-5). They more specifically argue that (1) "[n]othing in Pearson supports the examiner['s] unfounded assumption that the alert signal includes statistics (Reply Br. 4); (2) Pearson's wakeup signal does not have the claimed statistics (*id.*); and (3) transmission of a violated rule does not constitute communicating statistics (Reply Br. 4-5).

ISSUE

The issue before us is: Have Appellants shown the Examiner erred in finding that the cited prior art discloses or reasonably suggests a

communication process that communicates statistics collected in the gateway from the monitoring process to a control center?

FINDINGS OF FACT

The record supports the following Findings of Fact (FF) by a preponderance of the evidence:

1. The term "statistics" is defined as follows:

> 1. (*construed as sing.*) the science that deals with the collection, classification, analysis, and interpretation of numerical facts or data, and that, by use of mathematical theories of probability, imposes order and regularity on aggregates of more or less disparate elements. 2. (*construed as pl.*) the numerical facts or data themselves.

Webster's Encyclopedic Unabridged Dictionary of the English Language, 1389 (1989).

2. Pearson discloses a communication device that provides firewall functionality and intrusion-detection functionality for monitoring communications entering a local area network (LAN) and for determining whether such communications comprise an attack or other security risk (col. 7, l. 55-col. 8, l. 15). "More particularly, [the] intrusion detector [ ] inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list [ ] of known attack signatures" (col. 8, ll. 15-19). "Upon detecting an attack, the intrusion detector may then transmit an alert signal via the RMC communication module [ ] to indicate an intrusion has taken place or take other appropriate action" (col. 9, ll. 5-9).

PRINCIPLES OF LAW

To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *See In re Royka*, 490 F.2d 981, 985 (CCPA 1974). In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). If the Examiner's burden is met, the burden then shifts to Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006).

ANALYSIS

Before considering the rejections . . ., we must first [determine the scope of] the claims . . . ." *In re Geerdes*, 491 F.2d 1260, 1262 (CCPA 1974). Claim 1 recites, *inter alia*, a process of monitoring network traffic through a gateway and *communicating statistics* collected in the gateway from this monitoring process to a control center. Accordingly, we start the present inquiry by interpreting the meaning and scope of the disputed claim term, "statistics." Webster's Dictionary defines "statistics" as either "the science that deals with the collection, classification, analysis, and interpretation of numerical facts or data, and that, by use of mathematical theories of probability, imposes order and regularity on aggregates of more or less disparate elements;" or "the numerical facts or data themselves" (FF

1). The broadest reasonable interpretation of claim 1, then, requires that statistics, or numerical data used to interpret or analyze the network traffic, be communicated to a control center.

Pearson discloses a communication device that provides firewall functionality and intrusion-detection functionality for monitoring communications entering a local area network (LAN) and for determining whether such communications comprise an attack or other security risk (FF 2). "[The] intrusion detector [ ] inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list [ ] of known attack signatures" (*id.*). "Upon detecting an attack, the intrusion detector may then transmit an alert signal via the RMC communication module [ ] to indicate an intrusion has taken place or take other appropriate action" (*id.*).

We do not see how Pearson's communicating an alert signal from the communication device's intrusion detector to the RMC constitutes "communicating statistics." That is, we do not see how Pearson's transmitted alert signal constitutes "statistics," under the interpretation established *supra*. Although the alert signal will be composed of data (a series of 0s and 1s), the alert signal data is not "statistical" data. Rather, the alert signal data being communicated is merely a digital expression of a conclusion that an attack has occurred. This conclusion results from the intrusion detector—not the RMC—performing a statistical analysis of the underlying network data.

Applying this rationale to the rest of Pearson's disclosure, we likewise do not find a teaching of any other information communicated to RMC that can be construed as constituting "statistics." Furthermore, the Examiner

acknowledges that this limitation is not taught by Cheriton (Ans. 24-25). For the foregoing reasons, then, Appellants have persuaded us of error in the Examiner's obviousness rejection of independent claim 1. Accordingly, we will not sustain the Examiner's rejection of claim 1 or claims 2-15 which depend from claim 1.

Independent claim 16, which is directed to a method of protecting a victim site during a denial of service attack, recites limitations that are similar to those of claim 1: "monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics [sic: on the] network traffic; [and] communicating the statistics collected in the gateway to a control center . . . ."

Furthermore, independent claim 29 also sets forth that statistics are communicated to the control center:

> 29. A computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises [sic: comprising] instructions for causing a computer device coupled at an entry to the site to:
>
> monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic;
>
> communicate [sic: the] statistics[2] collected in the computer device to a control center; and

[2] We interpret the claim as intending to recite "the statistics." This interpretation is consistent with the Specification (Spec. 1-2) and avoids any question of whether the term possesses proper antecedent basis. That is, this interpretation clarifies that the communicated statistics are the same statistics that were provided from the heuristics measurements.

filter out packets that the device or control center deems to be part of an attack.

For the reasons set forth in relation to claim 1, Appellants have persuaded us of error in the Examiner's obviousness rejection of independent claims 16 and 29. Accordingly, we will not sustain the Examiner's rejection of those claims or claims 17-28 and 30-39 which respectively depend from claims 16 and 29.

CONCLUSIONS

Appellants have not contested the Examiner's non-statutory double patenting rejections of claims 1, 16, and 29 over either of Kaashoek or Poletto.

Appellants have shown the Examiner erred in finding that the cited prior art discloses or reasonably suggests a communication process that communicates statistics collected in the gateway from the monitoring process to a control center. Accordingly, Appellants have shown that the Examiner erred in rejecting claims 1-39 under 35 U.S.C. § 103.

DECISION

We summarily affirm the Examiner's decision rejecting claims 1, 16, and 29 for non-statutory double patenting over both of Kaashoek and Poletto.

We do not sustain the Examiner's obviousness rejection with respect to all pending claims on appeal. Therefore, the Examiner's decision rejecting claims 1-39 under 35 U.S.C. § 103 as obvious is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

ke

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis CA 95618